WHAT IS CLAIMED IS:

1. A method of processing financial transactions from a customer at an unmanned location, the method comprising:

acquiring identification information from the customer;

determining whether the customer has previously engaged in suspicious behavior or suspicious activity by comparing the customer's identification information to information stored in a suspicious persons database;

retrieving a score indicative of a level of suspicion if the customer has engaged in suspicious behavior or suspicious activity; and

authorizing financial transactions for the customer if the score is below a pre-selected threshold.

2. The method of Claim 1, wherein processing financial transactions comprises cashing a paper drafted check.

3. The method of Claim 1, wherein processing financial transactions at an unmanned location comprises processing financial transactions at an automatic teller machine (ATM).

4. The method of Claim 1, wherein acquiring identification information comprises acquiring at least one of a name, social security number, and a driver's license number.

5. The method of Claim 1, wherein acquiring identification information comprises acquiring biometric information of the customer.

6. The method of Claim 5, wherein the biometric information is an image.

7. The method of Claim 5, wherein comparing the customer's identification information to information stored in the database comprises comparing the customer's biometric information to previously stored biometric information in the suspicious persons database.

8. The method of Claim 7, wherein the method further comprises contacting a customer service agent if the customer's biometric information matches at least one of the previously stored biometric information in the suspicious persons database.

9. The method of Claim 8, wherein the method further comprises verifying the identity of the customer by the customer service agent if the customer's biometric information matches at least one of the previously stored biometric information in the suspicious persons database.

10. The method of Claim 9, wherein the method further comprises declining financial transactions for the customer if the customer service agent determines that the customer is engaging in suspicious behavior or suspicious activity.

11. The method of Claim 10, wherein the method further comprises contacting a customer service agent if the score is above the pre-selected threshold.

12. The method of Claim 11, wherein the method further comprises verifying the score by the customer service agent if the score is above the pre-selected threshold.

13. The method of Claim 12, wherein the method further comprises declining the financial transaction by the customer service agent if the score is above the pre-selected threshold.

14. A method of processing financial transactions at an unmanned location, wherein customers submit checks in exchange for cash, the method comprising:

acquiring information relating to the financial transactions and the customers;

creating records of customers that engage in suspicious behavior or suspicious activity, wherein the records comprise scores indicative of a level of suspicion; and

approving financial transactions from customers that have scores below a preset threshold of suspicious behavior or suspicious activity.

15. The method of Claim 14, wherein the method further comprises declining financial transactions from customers that have scores above a preset threshold of suspicious behavior or suspicious activity.

16. A method of identifying suspicious individuals in financial transactions at an unmanned location, the method comprising:

tracking suspicious individuals with scores indicative of a level of suspicion;

acquiring biometric information of the suspicious individuals;

storing the scores and the biometric information as records in a database;

identifying suspicious individuals when processing financial transactions by comparing either the biometric information or the scores to the suspicious individuals during financial transactions; and

declining financial transactions for suspicious individuals if the scores are above a pre-set threshold.

17. The method of Claim 16, wherein the method further comprises declining the transaction request if suspicious behavior or suspicious activity is suspected.

18. A method of processing financial transactions that transpire in an unmanned environment, the method comprising:

receiving transaction information from a plurality of customers;

creating records of customers that engage in suspicious behavior or suspicious activity;

identifying suspicious behavior or suspicious activity in financial transactions by comparing the received transaction information to the records so as to identify suspicious behavior or suspicious activity;

approving the financial transactions if suspicious behavior or suspicious activity is not suspected; and

declining financial transactions if suspicious behavior or suspicious activity is suspected.

19. The method of Claim 18, wherein creating records of customers comprises generating scores indicative of a level of suspicion.

20. The method of Claim 19, wherein creating records of customers comprises scoring the customers based on a degree of demonstrated suspicious behavior or suspicious activity.

21. A method of identifying suspicious behavior or suspicious activity in a financial transaction at an unmanned location, the method comprising:

receiving transaction requests from suspicious individuals and registered individuals at the unmanned location;

creating records of suspicious individuals having scores indicative of a level of suspicion;

comparing the scores of suspicious and registered individuals to a preset threshold of suspicion so as to identify suspicious behavior or suspicious activity;

approving the transaction requests if suspicious behavior or suspicious activity is not suspected; and

declining the transaction request if suspicious behavior or suspicious activity is suspected.

22. A system for processing financial transactions from customers at an unmanned location, the system comprising:

an interactive component positioned at the unmanned location, wherein the interactive component is configured to obtain transaction information relating to the financial transactions and the customers;

a storage component that records financial transactions of customers that demonstrate suspicious behavior or suspicious activity along with a score based on a level of suspicion and biometric information of the customer; and

a processing component that receives the transaction information from the interactive component and identifies suspicious behavior or suspicious activity relating to the financial transactions by either comparing the received transaction information to previously recorded scores or biometric information in the storage component.

23. The system of Claim 22, wherein the interactive component comprises an automatic teller machine (ATM).

24. The system of Claim 22, wherein the biometric information comprises an image.

25. The system of Claim 22, wherein the biometric information comprises a fingerprint.

26. The system of Claim 25, wherein the financial transaction involves cashing a check.

27. The system of Claim 26, wherein the transaction information comprises information on the check.

28. The system of Claim 22, wherein the storage component is a database.

29. The system of Claim 22, wherein the suspicious behavior or suspicious activity includes fraud.

30. A system for authorizing financial transactions at an unmanned location, wherein a customer submits a check in exchange for cash, the system comprising:

an input device positioned at the unmanned location, wherein the input device is configured to obtain check identification information from the check, identification information from the customer, and biometric information of the customer;

a database configured to store at least the biometric information; and

a processor configured to receive the identification information from the input device and identify suspicious behavior or suspicious activity relating to the customer prior to cashing the check by at least comparing the received biometric information to previously recorded biometric information in the database.

31. The system of Claim 30, wherein the processor determines whether the identification information corresponds to the biometric information in determining whether to accept or decline the check following receipt of at least one of the check identification information, the customer's identification information, and the customer's biometric information.

32. The system of Claim 31, wherein the processor determines whether the identification information identifies a customer that is authorized to cash checks on the account corresponding to the check.

33. The system of Claim 30, wherein the identification information comprises at least one of a social security number, a name, a driver's license number, a purchase amount, and an identification of the input device.

34. The system of Claim 30, wherein the check identification information comprises a MICR code.

35. The system of Claim 30, wherein the system further comprises a customer service agent that verifies the identity of the customer by using at least one of the check identification information, the customer's identification information, and the customer's biometric information.

36. A method of validating a financial transaction comprising:

receiving identification information from a customer at an unmanned location;

generating a biometric profile of the customer; and

identifying suspicious behavior or suspicious activity by comparing the generated biometric profile to previously stored biometric profiles of previous customers, wherein identifying suspicious behavior or suspicious activity occurs prior to authorizing the financial transaction.